

Abstract

One implementation of a method reassembles complete client-server conversation streams, applies decoders and/or decompressors, and analyzes the resulting data stream using multi-dimensional content profiling and/or weighted keyword-in-context. The method may detect the extrusion of the data, for example, even if the data has been modified from its original form and/or document type. The decoders may also uncover hidden transport mechanisms such as, for example, e-mail attachments. The method may further detect unauthorized (e.g., rogue) encrypted sessions and stop data transfers deemed malicious. The method allows, for example, for building 2 Gbps (Full-Duplex)-capable extrusion prevention machines.